

CLAIMS

1 1. Method for authenticating a portable object (7) comprising information
2 processing means (8) and information storage means (9, 10), the information storage means
3 containing at least one code (i) defining operations capable of being executed by the portable
4 object, as well as a one-way function, characterized in that it comprises the step that consists
5 of sending the portable object an order (31, 32i-34i, 35, 36) so that the latter executes a
6 calculation of a result by applying to said one-way function at least part of said code (i), this
7 result being used to decide whether or not the portable object is authentic.

1 2. Method according to claim 1, wherein said result enters into the
2 implementation of a given operation, this operation being performed successfully only when
3 the portable object (7) is authentic.

1 3. Method according to claim 2, wherein said given operation comprises a
2 decryption operation, said result making it possible to produce an associated decryption key.

1 4. Method according to claim 1, wherein said code part (i) used in the calculation
2 comprises a machine code part.

1 5. Method according to claim 1, wherein the portable object (7) contains a so-
2 called "real" code defining operations designed to be executed by the portable object, and a
3 so-called "dummy" code defining operations not designed to be executed by the portable
4 object, said code part used in the calculation comprising a dummy code part.

1 6. Method according to claim 1, wherein said order (31, 32i-34i, 35, 36) is sent to
2 the portable object repeatedly during its life, prior to the execution by the latter of said
3 operations.

1 7. Method according to claim 1, wherein said code part (i) used in the calculation
2 is defined by a start address (32i) and an end address (33i) in the information storage means,
3 said addresses being sent to the portable object.

1 8. Method according to claim 1, wherein said code (i) comprises a set of binary
2 words, said code part used in the calculation being defined by a subset of binary words
3 comprising the binary words distributed in the information storage means at a determined
4 pitch (34i), said pitch being sent to the portable object.

1 9. Method for having a portable object (7) execute a sensitive operation, the
2 portable object comprising information processing means (8) and information storage means
3 (9, 10), the information storage means containing at least one code (i) defining operations
4 capable of being executed by the portable object, as well as a one-way function, characterized
5 in that it comprises the step that consists of sending the portable object an order (31, 32i-34i,
6 35, 36) so that the latter executes a calculation of a result by applying to said one-way
7 function at least part of said code (i), said result entering into the implementation of said
8 sensitive operation, this operation being performed successfully only when the portable
9 object (7) is authentic.

1 10. Method according to claim 9, wherein said code part (i) used in the calculation
2 comprises a machine code part.

1 11. Method according to claim 9, wherein the portable object contains a so-called
2 "reel" code defining operations designed to be executed by the portable object, and a so-
3 called "dummy" code defining operations not designed to be executed by the portable object,
4 said code part used in the calculation comprising a dummy code part.

1 12. Portable object comprising information processing means (8) and information
2 storage means (9, 10), the information storage means containing at least one code (i) defining
3 operations capable of being executed by the portable object, as well as a one-way function,
4 characterized in that it comprises means for executing a calculation of a result by applying to
5 said one-way function at least part of said code.

1 13. Portable object according to claim 12, wherein said code part (i) used in the
2 calculation comprises a machine code part.

1 14. Device (1) comprising information processing means (2) and information
2 storage means (3, 4) and designed to communicate with a portable object (7) in order to
3 authenticate the latter, the portable object comprising information processing means (8) and
4 information storage means (9, 10), the information storage means of the portable object
5 containing at least one code (i) defining operations capable of being executed by the portable
6 object, as well as a one-way function, characterized in that it comprises means for sending the
7 portable object an order (31, 32i-34i, 35, 36) so that the latter executes a calculation of a
8 result by applying to said one-way function at least part of said code (i) of the portable object.

1 15. Device according to claim 14, wherein said code part (i) used in the
2 calculation comprises a machine code part.